PATENT ABSTRACTS OF JAPAN

(11)Publication number : **11-161167**
(43)Date of publication of application : **18.06.1999**

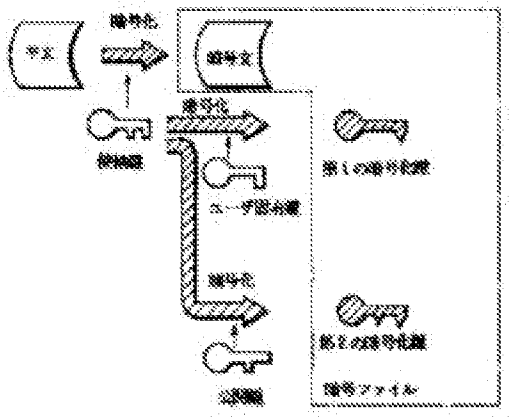
(51)Int.Cl. G09C 1/00
H04L 9/08

(21)Application number : **09-341951**
(22)Date of filing : **28.11.1997**

(71)Applicant : **PUMPKIN HOUSE:KK**
(72)Inventor : **SASAKI MINORU**

(54) DEVICE AND METHOD FOR CIPHERING AND RECORDING MEDIUM WHICH RECORDS CIPHERING PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To decode the ciphered sentence data, which are ciphered by a user, by a third party who is other than the user and is given a secret key.
SOLUTION: Every time plain sentence data are ciphered, a throwaway key is generated. Then, the data are ciphered employing the generated key and ciphered data are generated. Then, the throwaway key is ciphered by a user intrinsic key and an open key and first and second ciphering keys are generated. Then, the ciphered data and the first and the second ciphering keys are stored in a ciphering file. When a user deciphers the ciphered sentence data, the user obtains the throwaway key by decoding the first ciphering key using the user intrinsic key. If the third party, who is given a secret key, decodes the ciphered sentence data, the party obtains the throwaway key by decoding the second ciphered key using the secret key. Then, using the throwaway key, the ciphered sentence data are decoded into the plain sentence data.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－161167

(43)公開日　平成11年(1999)６月18日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０９Ｃ　1/00	６３０	Ｇ０９Ｃ　1/00	６３０Ｚ
			６３０Ａ
			６３０Ｅ
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｚ
			６０１Ａ

審査請求　未請求　請求項の数９　ＦＤ　（全　６　頁）　最終頁に続く

(21)出願番号　特願平9－341951

(22)出願日　平成９年(1997)11月28日

(71)出願人　393009356
株式会社パンプキンハウス
神奈川県厚木市飯山1620番地の１　アメニティヒル本厚木717

(72)発明者　佐々木　實
神奈川県厚木市飯山1620番地の１　アメニティヒル本厚木717　株式会社パンプキンハウス内

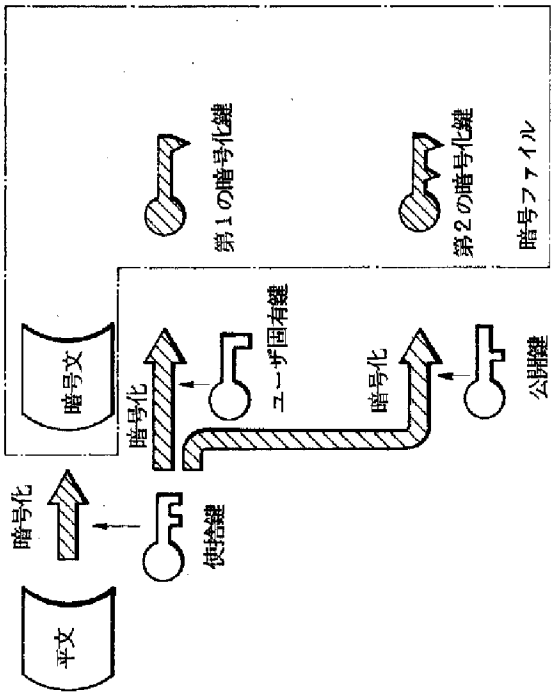
(74)代理人　弁理士　牛久　健司

(54)【発明の名称】　暗号化装置およびその方法ならびに暗号化プログラムを記録した記録媒体

(57)【要約】

【目的】　ユーザが暗号化した暗号文データをユーザ以外の秘密鍵を寄託された第三者が復号できるようにする。

【構成】　平文データを暗号化することに，使捨鍵を生成する。生成された使捨鍵を用いて平文データを暗号化し，暗号文データを生成する。使捨鍵をユーザ固有鍵および公開鍵で暗号化し，第１の暗号化鍵および第２の暗号化鍵を生成する。暗号文データ，第１の暗号化鍵および第２の暗号化鍵を暗号ファイルに格納する。ユーザが暗号文データを復号するときには，ユーザ固有鍵を用いて第１の暗号化鍵を復号することにより使捨鍵を得る。秘密鍵を寄託された第三者が暗号文データを復号するときには，秘密鍵を用いて第２の暗号化鍵を復号することにより使捨鍵を得る。使捨鍵を用いて暗号文データを平文データに復号する。



1

【特許請求の範囲】

【請求項１】　平文データを暗号化するために用いられるデータ暗号用鍵を用いて平文データから暗号文データを生成するデータ暗号化手段，上記データ暗号化手段において用いられるデータ暗号用鍵を，ユーザ固有鍵を用いて暗号化して第１の暗号化鍵を生成する第１の暗号化鍵生成手段，および上記データ暗号化手段において用いられるデータ暗号用鍵を，公開鍵を用いて暗号化して第２の暗号化鍵を生成する第２の暗号化鍵生成手段，を備えた暗号化装置。

【請求項２】　上記データ暗号用鍵を生成する暗号用鍵生成手段をさらに備え，上記データ暗号化手段が，上記暗号用鍵生成手段により生成されたデータ暗号用鍵を用いて上記平文データから上記暗号文データを生成するものである，請求項１に記載の暗号化装置。

【請求項３】　上記ユーザ固有鍵を生成するユーザ固有鍵生成手段をさらに備え，上記第１の暗号化鍵生成手段が，上記ユーザ固有鍵生成手段により生成されたユーザ固有鍵を用いて上記第１の暗号化鍵を生成するものである，請求項１に記載の暗号化装置。

【請求項４】　上記ユーザ固有鍵を用いて上記第１の暗号化鍵を復号し，上記データ暗号用鍵を得る第１の暗号化鍵復号手段，および上記第１の暗号化鍵復号手段による復号により得られた上記データ暗号用鍵を用いて上記暗号文データを平文データに復号するデータ復号手段，をさらに備えた請求項１に記載の暗号化装置。

【請求項５】　上記公開鍵に対応する秘密鍵を用いて上記第２の暗号化鍵を復号し，上記データ暗号用鍵を得る第２の暗号化鍵復号手段，および上記第２の暗号化鍵復号手段による復号により得られたデータ暗号用鍵を用いて暗号文データを平文データに復号するデータ復号手段，をさらに備えた請求項１に記載の暗号化装置。

【請求項６】　平文データを暗号化するために用いられるデータ暗号用鍵を用いて平文データから暗号文データを生成し，上記データ暗号用鍵を，ユーザ固有鍵を用いて暗号化して第１の暗号化鍵を生成し，上記データ暗号用鍵を，公開鍵を用いて暗号化して第２の暗号化鍵を生成する，暗号化方法。

【請求項７】　平文データを暗号化するために用いられるデータ暗号用鍵を用いて平文データから暗号文データを生成し，上記データ暗号用鍵を，ユーザ固有鍵を用いて暗号化して第１の暗号化鍵を生成し，上記データ暗号用鍵を，公開鍵を用いて暗号化して第２の暗号化鍵を生成するように暗号化装置のコンピュータを制御するためのプログラムを格納したコンピュータが読み取り可能な記録媒体。

【請求項８】　ユーザ固有鍵を用いて上記第１の暗号化鍵を復号して上記データ暗号用鍵を得，復号により得られたデータ暗号用鍵を用いて上記暗号文データを上記平文データに復号する，請求項７に記載のコンピュータが

2

読み取り可能な記録媒体。

【請求項９】　上記公開鍵に対応する秘密鍵を用いて，上記第２の暗号化鍵を復号して，上記暗号用鍵を得，復号により得られたデータ暗号用鍵で上記暗号文データを平文データに復号する，請求項７に記載のコンピュータが読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【技術分野】この発明は，暗号化装置および暗号化方法ならびにコンピュータが読み取り可能な記録媒体に関する。

【０００２】

【発明の背景】暗号装置における平文の暗号化および暗号文の復号には，共通鍵暗号システムによるものと，公開鍵暗号システムによるのとが知られている。

【０００３】共通鍵暗号システムでは，平文の暗号化に用いる鍵と暗号文の復号に用いる鍵とが同一である。

【０００４】公開鍵暗号システムでは，公開鍵を用いて平文を暗号化し，暗号化に用いられた鍵と対をなす秘密鍵を用いて暗号文を復号する。

【０００５】このような暗号システムにおいては政府から暗号文の復号のための鍵を要求された場合に，その要求に応じることが可能にすることが望まれている。

【０００６】

【発明の開示】この発明は，必要に応じて第三者が暗号文を復号できるようにすることを目的とする。

【０００７】この発明による暗号復号装置は，平文データを暗号化するために用いられるデータ暗号用鍵を用いて平文データから暗号文データを生成するデータ暗号化段，上記データ暗号化手段において用いられるデータ暗号用鍵を，ユーザ固有鍵を用いて暗号化して第１の暗号化鍵を生成する第１の暗号化鍵生成手段，および上記データ暗号化手段において用いられるデータ暗号用鍵を，公開鍵を用いて暗号化して第２の暗号化鍵を生成する第２の暗号化鍵生成手段を備えていることを特徴とする。

【０００８】この発明は，上記暗号化装置に適した方法も提供している。すなわち，平文データを暗号化するために用いられるデータ暗号用鍵を用いて平文データから暗号文データを生成し，上記データ暗号用鍵を，ユーザ固有鍵を用いて暗号化して第１の暗号化鍵を生成し，上記データ暗号用鍵を，公開鍵を用いて暗号化して第２の暗号化鍵を生成する暗号化方法である。

【０００９】この発明において平文データが暗号化された暗号文データを平文データに復号するときは，上記ユーザ固有鍵を用いて上記第１の暗号化鍵を復号し，上記データ暗号用鍵を得る。得られたデータ暗号用鍵を用いて暗号文データが平文データに復号される。

【００１０】上記ユーザ固有鍵は，通常は暗号文データを生成したユーザが管理する。上述のようにユーザは，上記ユーザ固有鍵を用いて暗号文データを平文データに

復号できる。

【００１１】上記秘密鍵は，通常は，メーカ，販売店が管理し，メーカ，販売店から寄託された第三者は，上記秘密鍵を用いて暗号文データを平文データに復号できる。

【００１２】平文データを暗号文データに暗号化するときに用いられるデータ暗号用鍵は，平文データを暗号化するごとに新たに生成されるような上記使捨鍵であることが好ましい。暗号化されるごとに使捨鍵が生成され，生成された使捨鍵を用いて平文データが暗号化されるので，特定の暗号用鍵を用いて暗号文データを生成する場合に比べ復号する権限のない者により暗号文データが復号されてしまう危険を低くできる。このため暗号文データの機密性を向上させることができる。

【００１３】上記データ暗号用鍵または上記ユーザ固有鍵を生成し，生成された上記データ暗号用鍵またはユーザ固有鍵を用いて上記平文データから暗号文データを生成してもよい。

【００１４】

【実施例の説明】図１は，この実施例による暗号化復号装置の電気的構成を示すブロック図である。

【００１５】暗号化復号装置は，コンピュータ１を含む。コンピュータ１にはデータを表示するための表示装置２，バスを介して入力を受け付けるための入力装置（キーボード，マウスなど）３，データを一時記憶するための外部記憶装置４，ならびにフロッピィ・ディスクＦＤに記録されたデータを読みとり，かつＦＤにデータを記録する第１のＦＤドライブ５および第２のＦＤドライブ６が接続されている。

【００１６】暗号化復号装置においては，暗号化復号装置のユーザが平文データを暗号化し，暗号化によって得られた暗号文データをユーザが復号できるとともに，ユーザ以外の特定の秘密鍵を寄託された第三者が暗号文データを復号できる。

【００１７】図２は，暗号化復号装置によって実行される暗号化処理の概要を鍵の働きを中心に示すものである。図３は，ユーザによって実行される復号処理の概要を鍵の働きを中心に示すものであり，図４は，ユーザ以外の秘密鍵を寄託された第三者によって実行される復号処理の概要を鍵の働きを中心の示すものである。図５および図６は，ユーザによって実行される暗号化復号処理の手順を示すフローチャート，図７は，秘密鍵を寄託された第三者によって実行される復号処理の手順を示すフローチャートである。

【００１８】まずユーザによって実行される暗号化復号処理について説明する。

【００１９】図１，図２，図５および図６を参照して，ユーザによって第１のＦＤドライブ５に暗号化復号プログラムが格納された第１のＦＤが装着される。第１のＦＤドライブ５に装着された第１のＦＤが初期化されているかどうかが判定される（ステップ１１）。

【００２０】第１のＦＤが初期化されていなければ（ステップ１１でNO），入力装置３からユーザの名前が入力される（ステップ１２）。また，第１のＦＤから読みとられた暗号化復号プログラムにしたがってコンピュータ１において第１の乱数および第２の乱数が生成される（ステップ１３）。

【００２１】入力装置３から入力された名前を表すデータと生成された第１の乱数を表すデータとがユーザ固有のIDとされる（ステップ１４）。また，第２の乱数がユーザ固有鍵とされる（ステップ１５）。

【００２２】ステップ１２から１５の処理によりＦＤの初期化が終了する。

【００２３】第１のＦＤドライブ５に装着された第１のＦＤがすでに初期化されていると（ステップ１１でYES），ステップ１２から１５の処理はスキップされる。

【００２４】ＦＤの初期化処理が終了する，または初期化済みのＦＤが第１のＦＤドライブ５に装着されると，外部記憶装置４に記憶されているファイルが読み込まれる（ステップ１６）。読み込まれたファイルが平文データを表すものかどうかが判断される（ステップ１７）。平文データであれば（ステップ１７でYES），暗号化処理が実行される（ステップ１８から２２）。平文データでなければ（ステップ１７でNO），復号処理が実行される（ステップ２３から２６）。

【００２５】平文データの暗号化を実行する場合には，暗号化に用いる使捨鍵を生成するために乱数が生成される（ステップ１８）。生成された乱数が使捨鍵となる。生成された使捨鍵を用いて外部記憶装置４から読み出された平文データが暗号化される。この暗号化により暗号文データが生成される（ステップ１９）。

【００２６】生成されたユーザ固有鍵を用いて使捨鍵が暗号化される（ステップ２０）。ユーザ固有鍵を用いて使捨鍵が暗号化されることにより第１の暗号化鍵が生成される。

【００２７】さらに，第１のＦＤに記憶されている暗号化復号プログラムにもとづいて公開鍵が読み出される。読み出された公開鍵を用いて使捨鍵が暗号化される（ステップ２１）。公開鍵を用いて使捨鍵が暗号化されることにより第２の暗号化鍵が生成される。

【００２８】ユーザID，第１の暗号化鍵，第２の暗号化鍵および暗号文データが暗号ファイルとして外部記憶装置４に格納される（ステップ２２）。また第１のＦＤに記憶されている暗号化復号プログラムのバージョンを表す情報も暗号ファイルに記憶される。

【００２９】次に生成された暗号文データをユーザが復号する処理について説明する。ユーザによる復号も，第１のＦＤに記憶されている暗号化復号プログラムにしたがって実行される。

【００３０】主に図３および図６を参照して外部記憶装

置４から暗号ファイルが読み出される（ステップ１７でNO）。暗号ファイルが読み出されると，ユーザは入力装置３からユーザIDを入力する。暗号ファイルに格納されているバージョン情報およびユーザIDと，第１のＦＤに記憶されているバージョン情報およびユーザが入力したユーザIDとが一致するかどうかが判断される（ステップ２３）。

【００３１】一致すると，第１のＦＤに記憶されているユーザ固有鍵を用いて第１の暗号化鍵が復号される（ステップ２４）。これにより平文データを暗号化するのに用いられた使捨鍵が生成される。

【００３２】使捨鍵が生成されると，生成された使捨鍵を用いて暗号文データが平文データに復号される（ステップ２５）。生成された平文データは表示装置２に与えられ，平文データによって表される平文が表示装置上に表示される（ステップ２６）。

【００３３】バージョン情報およびユーザIDが一致しないと（ステップ２３でNO），そのバージョン情報が格納されている暗号ファイルに含まれる暗号文データを復号できずに表示装置４にエラーが表示される（ステップ２３）。

【００３４】この実施例による暗号化復号装置は，暗号化を実行したユーザが暗号文データを復号することができるだけでなく，ユーザ以外の秘密鍵を寄託された第三者もユーザが暗号化した暗号文データを復号することができる。

【００３５】次にユーザによって暗号化された暗号文データを秘密鍵を寄託された第三者が復号する場合について説明する。

【００３６】ここでは，図１に示す暗号化復号装置を用いて秘密鍵を寄託された第三者が暗号文データを平文データに復号するものとする。もちろん，秘密鍵を寄託された第三者が有する復号装置を用いて暗号文データを復号することができるのはいうまでもない。公開鍵方式による復号プログラムおよび暗号化復号装置において第２の暗号化鍵の生成に用いられた公開鍵に対応する秘密鍵が記憶されているＦＤが第２のＦＤドライブ６に装着される。第２のＦＤドライブ６に装着されたＦＤに記憶されている復号プログラムにしたがって復号処理が実行される。

【００３７】図４および図７を参照して，外部記憶装置４に暗号ファイルが記憶されている。外部記憶装置４から暗号ファイルが読み出され（ステップ３１），読み出されたファイルが暗号文データかどうかが判断される（ステップ３２）。

【００３８】暗号ファイルの場合（ステップ３２），暗号ファイルに記憶された暗号プログラムのバージョン情報とユーザIDが，復号プログラムのバージョン情報とユーザIDと一致するかどうかが判定される（ステップ３３）。

【００３９】一致すると（ステップ３４），暗号ファイルに記憶されている第２の暗号化鍵が読み出される。また第２のＦＤに記憶されている秘密鍵が読み出される。第２のＦＤから読み出された秘密鍵を用いて，暗号ファイルから読み出された第２の暗号化鍵が復号される（ステップ３４）。これにより平文データを暗号文データに暗号化するときに用いられた使捨鍵が生成される。

【００４０】暗号ファイルから暗号文データが読み出され，生成された使捨鍵を用いて暗号文データが復号される（ステップ３５）。この復号により平文データが生成される。

【００４１】生成された平文データによって表される平文が表示装置４に表示される（ステップ３６）。暗号文データを生成したユーザが暗号文データを平文データに復号するためのユーザ固有鍵がわからなくなってもユーザ以外の秘密鍵を寄託された第三者が暗号文データを復号することができる。

【００４２】暗号ファイルから読み出した暗号文データを生成したときの暗号化プログラムのバージョンと第２のＦＤドライブ６に装着された第２のＦＤに記憶されている復号プログラムのバージョンとが一致しないときには復号ができない。このときには，表示装置４には復号ができないことを示すエラーが表示される（ステップ３７）。

【００４３】上述の実施例においては，暗号ファイルは外部記憶装置４に記憶されているが，ＦＤに記憶するようにしてもよい。

【００４４】また，秘密鍵を寄託された第三者による暗号文データの復号は公開鍵方式を用いているので，暗号文データの機密性を高く保持することができる。

【図面の簡単な説明】

【図１】暗号化復号装置の電気的構成を示すブロック図である。

【図２】暗号化の概要を示す。

【図３】ユーザによる復号の概要を示す。

【図４】ユーザ以外の秘密鍵を寄託された第三者による復号の概要を示す。

【図５】ユーザによる暗号化復号処理の手順を示すフローチャートである。

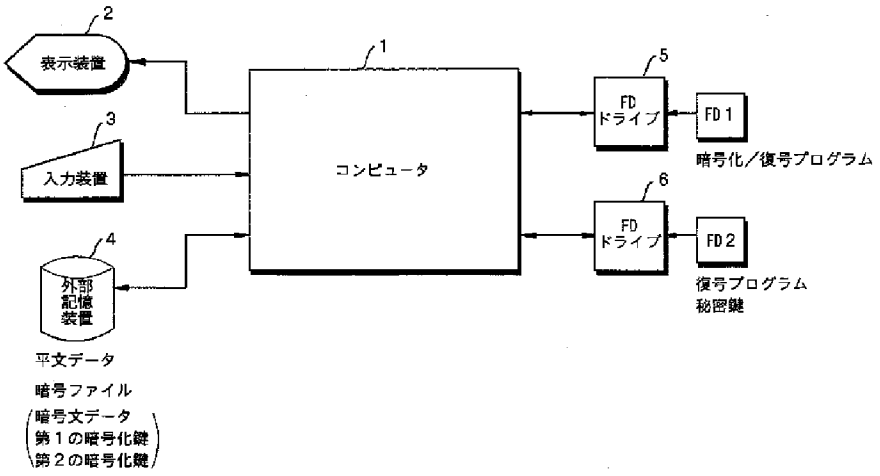
【図６】ユーザによる暗号化復号処理の手順を示すフローチャートである。

【図７】秘密鍵を寄託された第三者による復号処理の手順を示すフローチャートである。

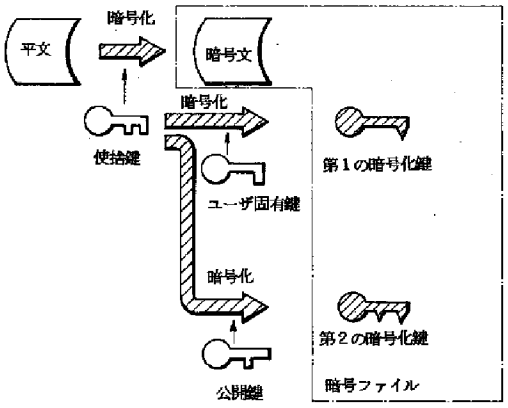
【符号の説明】

１　コンピュータ
２　表示装置
３　入力装置
４　外部記憶装置
５，６　ＦＤドライブ

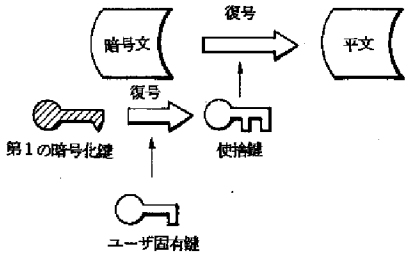
【図１】


2
表示装置
1
5
FD
ドライブ
FD１
暗号化／復号プログラム
3
入力装置
コンピュータ
6
FD
ドライブ
FD２
復号プログラム
秘密鍵
4
外部
記憶
装置
平文データ
暗号ファイル
暗号文データ
第１の暗号化鍵
第２の暗号化鍵

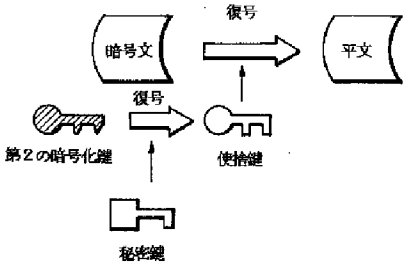
【図２】


平文
暗号化
暗号文
使捨鍵
暗号化
第１の暗号化鍵
ユーザ固有鍵
暗号化
第２の暗号化鍵
公開鍵
暗号ファイル

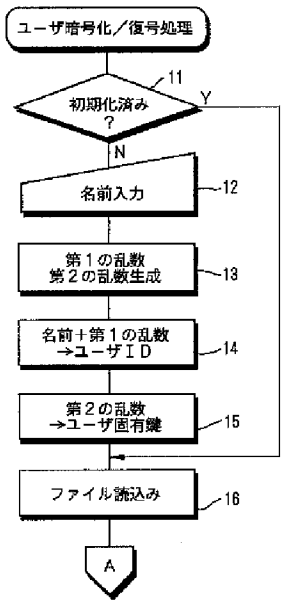
【図３】


暗号文
復号
平文
復号
第１の暗号化鍵
使捨鍵
ユーザ固有鍵

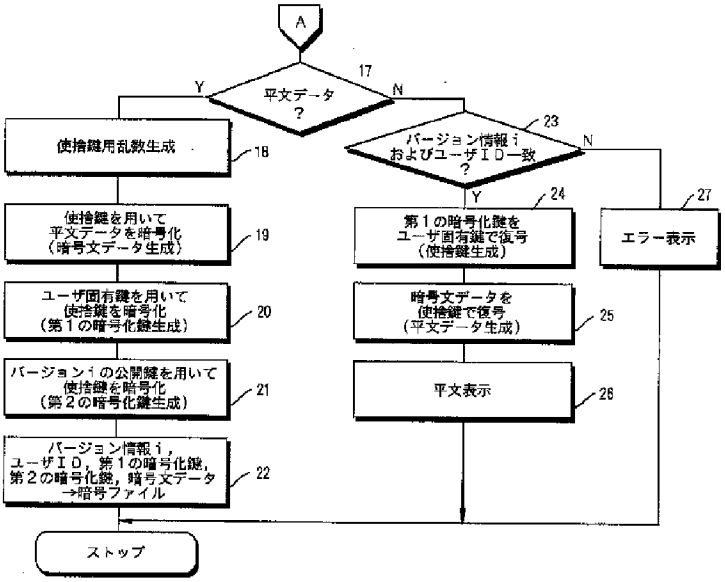
【図４】


暗号文
復号
平文
復号
第２の暗号化鍵
使捨鍵
秘密鍵

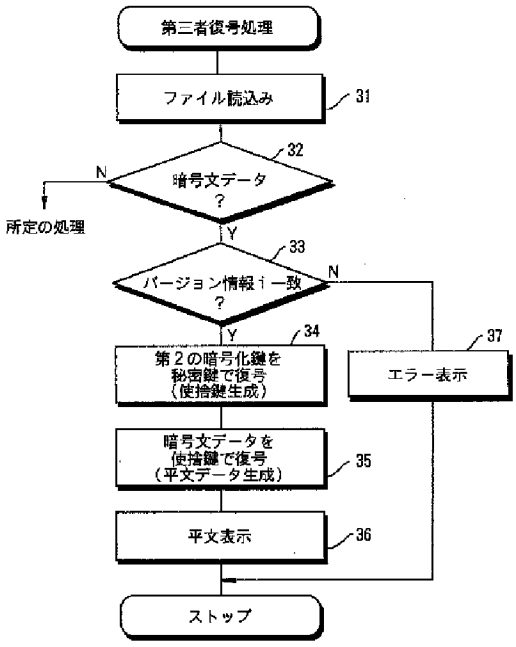
【図５】


ユーザ暗号化／復号処理
11
初期化済み
？
Y
N
名前入力
12
第１の乱数
第２の乱数生成
13
名前＋第１の乱数
→ユーザＩＤ
14
第２の乱数
→ユーザ固有鍵
15
ファイル読込み
16
A

【図６】



【図７】



フロントページの続き

(51)Int.Cl.[6]	識別記号	ＦＩ
		Ｈ０４Ｌ　9/00　　６０１Ｅ